CWIN

Critical infrastructure Warning Information Network

Protecting Critical Infrastructures

Protecting critical infrastructure and key assets is one of the Department of Homeland Security's critical mission areas. Since private industry owns and operates approximately 85% of our critical infrastructures, Government and industry must work together in this mission.

Established originally with a focus on protecting the Nation's cyber infrastructures, CWIN supports critical infrastructure protection across all sectors. It provides a private, protected and reliable network, offering voice and data connectivity to Government and industry partners. Membership is distributed through all the critical infrastructure sectors, and, when complete, will include Government, industry and information and sharing analysis centers for each sector.

A Collaboration and Alert Notification Tool

CWIN provides a reliable and survivable network capability and has no logical dependency on the Internet or the Public Switched Network (PSN). As a result, if either the Internet or PSN suffer degradations, CWIN will not be affected. Operating 24x7, CWIN is always available for communicating important alerts and advisories, sharing information and working with Government and other partners both within and among the critical sectors.

Thin Client Terminals

CWIN employs a thin client-server-based computing environment. CWIN system administrators configure and update all CWIN members' terminals from a centralized data location. Thin client technology offers:

Data Security: No data is present on the desktop. All user data resides on remote servers. There is no data loss if the terminal is stolen or destroyed. User profiles are created upon logon and deleted at log off.

Small Footprint: The desktop requires less physical space than the traditional PC. This is ideal for use with multiple network/desktop requirements in limited spaces.

Protecting the Nation's critical infrastructures through reliable communications

Voice over Internet Protocol (VoIP) Phones

The NCS selected a VoIP phone network for CWIN because it provides security, reliability, scalability and dynamic re-routing capability. VoIP telephony technology enables the transmission of voice signals digitally in discrete packets, avoiding the need for the dedicated circuits required by traditional analog telephony.

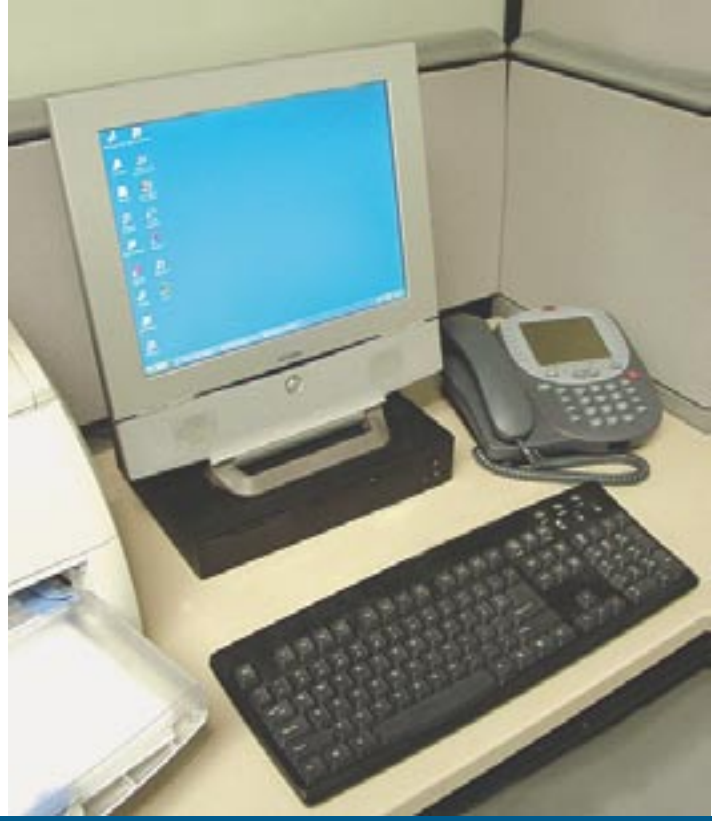
The backbone is an IP-enabled virtual private network (VPN) and is not susceptible to the potential service delays that result from high traffic volumes that occur during an emergency or Signaling System Seven (SS7) interruption. CWIN's architecture includes secure data centers, private branch exchanges (PBXs), and private lines for redundant and reliable connectivity.

Critical Sectors

- Banking & Finance
- Chemical & HAZMAT
- Postal & Shipping
- Continuity of Government
- Key Resources
- Agriculture
- Food
- Water
- Public Health
- Emergency Services
- Defense Industrial Base
- Telecom
- Information Technology
- Energy
- Transportation

The Mission of CWIN

The Critical infrastructure Warning Information Network (CWIN) serves to facilitate immediate alert, notification, sharing and collaboration of critical infrastructure and cyber information within and between Government and industry partners.



Department of Homeland Security
National Communications System

Attention: CWIN Program Manager
701 South Courthouse Road
Arlington, VA 22204-2198

Tel: 1-866-NCS-CALL (1-866-627-2255)

E-mail: cwin@ncs.gov

Web: http://www.ncs.gov/

CWIN

Critical infrastructure Warning Information Network

National Communications System